PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on January 11, 2006.

Robert J. Lorch

Applicant	: Craig L. Ogg et al.	Confirmation No. 2004
Application No.	: 09/690,083	
Filed	: October 16, 2000	
Title	: CRYPTOGRAPHIC MODULE FOR SECURE PROCESSING OF VALUE-BEARING ITEMS	
Grp./Div.	: 3621	
Examiner	: Firmin Backer	
Docket No.	: 40630/S850	

SUBMISSION OF APPELLANT'S BRIEF
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Post Office Box 7068
Pasadena, CA 91109-7068
January 11, 2006

Commissioner:

Enclosed for filing is the Appellant's Brief for this application.

_____ An extension of time to file Appellant's Brief is requested, and a Petition for Extension of Time and the applicable fee are enclosed.

__X__ Our check for $500 to cover the fee for the appeal brief is enclosed.

_____ An oral hearing of the appeal is requested, and our check for $_, the fee for the oral hearing, is enclosed.

The Commissioner is hereby authorized to charge any further fees under 37 CFR 1.16 and 1.17 which may be required by this paper to Deposit Account No. 03-1728. Please show our docket number with any charge or credit to our Deposit Account. **A copy of this letter is enclosed.**

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By _____

Jonathan S. Miller
Reg. No. 48,534
626/795-9900

JSM/rjl
RJL PAS661294.1-*-01/11/06 3:45 PM

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on January 11, 2006.

Robert I. Lorch

Applicants	:	Craig L. Ogg et al.	Confirmation No. 2004
Application No.	:	09/690,083	
Filed	:	October 16, 2000	
Title	:	CRYPTOGRAPHIC MODULE FOR SECURE PROCESSING OF VALUE-BEARING ITEMS	
Grp./Div.	:	3621	
Examiner	:	Firmin Backer	
Docket No.	:	40630/S850	

APPELLANTS' BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Post Office Box 7068
Pasadena, CA 91109-7068
January 11, 2006

Commissioner:

Applicants, (hereinafter "Appellants") submit the following Appeal Brief pursuant to 37 C.F.R. § 41.37 for consideration by the Board of Patent Appeals and Interferences. Appellants also submit herewith a check in the amount of $500.00 to cover the cost of filing the opening brief as required by 37 C.F.R. § 41.20(b)(2). Please charge any additional amount due or credit any overpayment to deposit Account No. 03-1728.

1. REAL PARTY IN INTEREST

Craig L. Ogg and William W. Chow, the parties named in the caption, assigned their rights to the invention disclosed in the subject application through an Assignment recorded on February 01, 2001 at reel and frame 011489/0616 to Stamps.com, 3420 Ocean Park Boulevard, Suite 1040, Santa Monica, California 90405. Therefore, Stamps.com is the real party in interest.

2. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this Appeal.

3. STATUS OF CLAIMS

Claims 1-120 stand rejected. Appellants appeal the rejection of claims 1-120.

4. STATUS OF AMENDMENTS

No amendments to the claims were submitted after the Office Action mailed August 2, 2005.

5. SUMMARY OF CLAIMED SUBJECT MATTER

The subject matter of claim 1 relates to a cryptographic device for securing data on a computer network. See page 3, lines 5-24. The cryptographic device includes a processor programmed to authenticate a plurality of users on the computer network for secure processing of a value bearing item, wherein the processor includes a state machine for determining a state corresponding to availability of one or more commands. Figure 3, page 4, lines 10-20, page 11, line 32 - page 12, line 10, page 12, lines 23-30, and page 42, lines 28-35. The device includes memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users. Page 6, line 30 - page 7, line 10. The device includes a cryptographic engine for cryptographically protecting data. Page 12, line 23 - page 15, line 35. The device includes an interface for communicating with the computer network. Page 12, lines 27-30. The cryptographic device is located remotely

from the plurality of users. Page 7, lines 11-14. Once the user is authenticated, the cryptographic device enters an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user. Page 43, lines 21-29 and page 47, line 12 - page 48, line 25.

The subject matter of claim 42 relates to a method for securing data on a computer network including a plurality of remotely-located users. The method includes authenticating the plurality of users for secure processing of a value bearing item using one of a plurality of cryptographic devices. Page 3, line 33 - page 4, line 9. The method includes storing security device transaction data in a memory for ensuring authenticity and authority of one of the plurality of users, wherein the security device transaction data is related to the one of the plurality of users. Page 6, line 30 - page 7, line 10. The method includes determining a state in a state machine for availability of one or more commands. Page 42, lines 28-35. Once the user is authenticated, an operational state is entered in which it continues to authenticate the user with respect to one or more transactions requested by the user. Page 43, lines 21-29 and page 47, line 12 - page 48, line 25.

The subject matter of claim 72 relates to a security system for securing data in a computer network. See page 3, lines 5-24. The system includes a plurality of user terminals coupled to the computer network. The system includes a plurality of cryptographic devices remote from the plurality of user terminals and coupled to the computer network, wherein one of the plurality of cryptographic devices manages value available to users and includes a state machine for determining a state corresponding to one or more commands available to an authenticated user. Page 4, lines 10-20, page 11, line 32 - Page 12, line 10, and Figure 3; page 12, lines 23-30, page 42, lines 28-35. The system includes a plurality of security device transaction data for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user. Page 6, line 30 - page 7, line 10. Once the user is authenticated, the cryptographic device enters an operational state in which it continues to authenticate the user for one or more transactions requested by the user. Page 43, lines 21-29 and page 47, line 12 - page 48, line 25.

The subject matter of claim 104 relates to a method for secure printing of value-bearing items over a computer network having a plurality of user terminals. The method includes storing information about a plurality of users using the plurality of terminals in a database remote from the plurality of user terminals. Page 3, lines 14 - 23. The method includes securing the information about the users in the database by one or more of a plurality of cryptographic devices remote from the plurality of user terminals, wherein each of the cryptographic devices

manages value available for the value bearing items. Page 7, line 33 - page 8, line 13. The method includes storing a plurality of security device transaction data in the database, wherein each transaction data is related to one of the plurality of users. Page 6, line 30 - page 7, line 10. The method includes determining a state in a state machine for availability of one or more commands and continuing to authenticate individual user transaction requests even after a user has been authorized by the cryptographic device. Page 42, lines 28-35, page 43, lines 21-29 and page 47, line 12 - page 48, line 25.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-120 are rejected as unpatentable under 35 U.S.C. §103 as allegedly being obvious over U.S. Patent No. 6,424,954 issued to Leon ("Leon") in view of U.S. Patent No.6,546,377 issued to Gravell ("Gravell").

7. ARGUMENT

A. Rejection of Claims 1-120 as Obvious Under 35 U.S.C. § 103 based on Leon in view of Gravell

Claim 1 stands rejected under 35 U.S.C. § 103 based on Leon in view of Gravell. Appellants believe that the Examiner has failed to establish that the cited references teach or suggest each of the elements of these claims and believe the Examiner has improperly combined these references.

To establish a *prima facie* case of obviousness the Examiner must show that the cited references teach or suggest each of the elements of the claim. In regard to independent claim 1, this claim recites a cryptographic device that includes "a processor programmed *to authenticate a plurality of users on the computer network* for secure processing of a value bearing item, wherein the processor includes a state machine for determining a state corresponding to availability of one or more commands" (emphasis added) and "wherein the cryptographic device is located remotely from the plurality of users."

Appellants have reviewed the cited sections of Leon but have been unable to discern any part therein that teaches these elements of claim 1. Rather, the cited sections of Leon, for example figs. 1A and 1B, cited as teaching the computer network, show a system with a secure meter device (SMD) 150 in communication via an RS-232 cable (Reference No. 122) with a single Personal Computer (PC) 120. The SMD of Leon as shown in Figs. 1A and 1B is a discrete localized hardware device connected to and associated with a single user's PC. The device is housed in a tamper-proof case and located in close proximity to the user's PC such that a printer, a scale or a similar device can be directly coupled to the SMD. Thus, the system taught by Leon is based on the use of an individual SMD device that is directly coupled to each user PC. This necessitates the use of hundreds or thousands of SMD devices to service users, where an SMD is needed for each user machine. The system of Leon is the antithesis of a remote cryptographic device that authenticates a plurality of users, as recited in claim 1.

Thus, it is unclear to the Appellants how Leon, and specifically these figures cited by the Examiner, teaches a remote cryptographic device and a processor that is able to "authenticate a plurality of users on the computer network." The SMD of Leon has not been shown by the Examiner to support a plurality of users or to operate on a computer network.

The sections of Leon that the Examiner cites for supporting the assertion that a processor including "the state machine for determining a state corresponding to availability of one or more commands" is taught by Leon all discuss the SMD. See the Abstract, figures 5A-7, and column 9 lines 35-67 of Leon, which were cited by the Examiner. However, the Appellants have reviewed these sections of Leon, but have been unable to discern any part therein that discloses that the SMD of Leon includes a processor that supports a state machine, as recited in claim 1. Thus, the Examiner has not established that the SMD of Leon teaches or suggests each of the elements of claim 1.

The Examiner's use of Leon as a reference and basis for rejecting claim 1 is unclear in Paper no. 7. The Examiner has confusingly stated that "Leon *fails to teach a system programmed to authenticate a plurality of user* (*sic*) for secure processing if *(sic)* a value bearing item and memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users and a

the (*sic*) cryptographic module is remotely located from the user wherein once the user is authenticated (*sic*) (Emphasis added)." See page 3 of Paper no. 7, middle of the paragraph. This appears to contradict earlier statements in Paper no. 7, where the Examiner relied on Leon to teach the elements of claim 1, stating "Leon teaches a cryptographic device (*SMD, 110a, 110b comprise a cryptographic module*) for securing data on a computer network ... comprising a processor ... programmed to authenticate ... users ... on the computer network." See Paper no. 7, page 3 start of the first paragraph.

Further, the Examiner has not established that Gravell cures the defects of Leon. The sections of Gravell cited by the Examiner in Paper no. 7 do not appear to teach a processor in a cryptographic device as recited in the independent claims. Rather, Gravell teaches a system with multiple servers, where separate servers, each with their own independent processors, handle different functionality. See Figure 1 and col. 7, lines 21-37 of Gravell. Specifically, a function server "supports ... postage dispensing and postal reporting" while "sensitive cryptographic processes occur in the Key Management System 38." Thus, Gravell does not teach a system with a cryptographic device having a processor "to authenticate a plurality of users ... for secure processing of a value bearing item" and having a "cryptographic engine for cryptographically protecting data." Rather, Gravell discloses a system where these functions are performed by separate servers, a function server and a key management server. Figure 1 and col. 7, lines 21-37 of Gravell.

Also, the Examiner has not identified and Appellants have been unable to discern any part of Gravell that teaches a cryptographic device having a processor that "includes a state machine for determining a state corresponding to availability of one or more commands." Thus, Gravell does not cure the defects of Leon and the references, combined, fail to teach or suggest each of the elements of claim 1.

Further, the Appellants believe the proposed combination of Gravell with Leon is not suggested by the references and would change the principle of operation of Leon, which is the primary reference. The prior art must suggest the desirability of the claimed invention. Also, the proposed modification or combination of the prior art cannot change the principle of operation of

the prior art invention being modified. See MPEP § 2143.01. Therefore, Gravell has been improperly combined with Leon.

As discussed above, Leon teaches a system with a specialized secure meter device that maintains a set of security relevant data items (SRDIs) such as revenue registers and cryptographic keys and performs the secure processing required by a postage metering system. See column 4, lines 44-49 of Leon. The SMD and postal metering system are housed in a tamper-proof case that is located in close proximity to the host PC such that a printer, scale or similar peripheral device can be directly plugged into the postage meter system and SMD of Leon. See Figures 1A, 1B, 2A, 2B, 3A and 3B and column 2, lines 49-52 and column 4, lines 3-7 of Leon.

As discussed above, the Examiner seeks to cure the defects of Leon by modifying Leon in view of Gravell. However, Gravell explicitly teaches away from such a combination with Leon, also, this combination would change the operating principle of Leon. Gravell teaches a system utilizing a virtual postage metering system that is accessed at a remote data center. Gravell states that its system is specifically designed to avoid the use of physical meters such as those taught in Leon. See column 4, lines 4-12 of Gravell. Thus, one of ordinary skill in the art would not think to combine the virtual system of Gravell with the physical meter system of Leon, because Gravell teaches away from the use of a physical meter system.

Further, the proposed modification of Leon to place the physical meter of Leon at a remote location or to somehow modify the physical meter of Leon to be virtual in the manner of the Gravell system changes the principle of operation for Leon by making it a virtual system as opposed to a physical meter system and renders Leon unfit for its intended purpose. By making the postage metering system of Leon remote from the user, the user is not able to locally access or use the physical meter of Leon in combination with a scale plugged in to the physical meter or in combination with a printer that is part of the physical meter as taught by Leon. Thus, combining the virtual system of Gravell, which is executed on the remote data center, with the physical postage device of Leon is improper. Therefore, the Examiner has improperly combined Leon and Gravell. Accordingly, it is requested that the obviousness rejection of claim 1 be overturned.

In regard to claims 6 and 7, these claims depend from independent claim 1 and incorporate the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 1, these claims are not obvious over Leon in view of Gravell. In addition, these claims include the elements of "an exporting shares state" and "an importing shares state." The sections of Leon relied upon by the Examiner do not mention such states or the use of shares. Thus, Appellants believe the Examiner has failed to establish that these elements of claims 6 and 7 are taught or suggested by the cited references. Accordingly, it is believed these claims are separately patentable and it is requested that the obviousness rejections of these claims be overturned.

In regard to claim 11, this claim depends from independent claim 1 and incorporates the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 1, this claim is not obvious over Leon in view of Gravell. In addition, this claim includes the elements of "one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support." The Examiner cites col. 11, lines 36-43 of Leon as teaching these elements of claim 11. However, the cited section makes no mention of any of these commands, or any commands that correspond to an operations state. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claim 11. Accordingly, it is believed that this claim is separately patentable and it is requested that the obviousness rejection of this claim be overturned.

In regard to claim 12, this claim depends from independent claim 1 and incorporates the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 1, this claim is not obvious over Leon in view of Gravell. In addition, this claim includes the elements of "wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access control database command, change password command, set clock command, and set Status command." The Examiner cites fig. 5b and col. 13, line 63 - col. 14, line 31 of Leon as teaching these elements of claim 12. However, the cited sections make no mention of any of these commands. Rather, the cited sections of Leon relate to an Initialization transaction and Registration transaction. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claim 12. Accordingly, it is believed

that this claim is separately patentable and it is requested that the obviousness rejection of this claim be overturned.

In regard to claim 13, this claim depends from independent claim 1 and incorporates the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 1, this claim is not obvious over Leon in view of Gravell. In addition, this claim includes the elements of "wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session MAC command, session encrypt command, and session decrypt command." The Examiner cites col. 13, lines 36-62 of Leon as teaching these elements of claim 13. However, the cited sections make no mention of any of these commands or any commands that correspond to session management. Rather, the cited section of Leon relates to an Initialization transaction. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claim 13. Accordingly, it is believed that this claim is separately patentable and it is requested that the obviousness rejection of this claim be overturned.

In regard to claim 16, this claim depends from independent claim 1 and incorporates the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 1, this claim is not obvious over Leon in view of Gravell. In addition, this claim includes the elements of "wherein the one or more commands corresponding to the administrative state include commands for one or more of create account command, delete account command, modify account command, view access control database command, end admin. command, logon command, logoff command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command." The Examiner cites figs. 5a-7 and col. 9, lines 35-672 of Leon as teaching these elements of claim 16. However, the cited sections make no mention of any of these commands or any commands that correspond to an administrative state. Rather, the cited sections of Leon relate to other operating states. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claim 16. Accordingly, it is believed that this claim is separately patentable and it is requested that the obviousness rejection of this claim be overturned.

In regard to claim 17, this claim depends from independent claim 1 and incorporates the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 1, this claim is not obvious over Leon in view of Gravell. In addition, this claim includes the elements of "wherein the one or more commands corresponding to the exporting shares state include commands for one or more of logon command, logoff command, query Current User Role command, query current user ID command, export share command, abort export command, get status command, session management commands, and audit entry creation command." The Examiner cites col. 8, line 63 - col. 9, line 19 of Leon as teaching these elements of claim 17. However, the cited section makes no mention of any of these commands or any commands that correspond to exporting shares. Rather, the cited section of Leon relates to initialization transactions performed by a crypto-officer. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claim 17. Accordingly, it is believed that this claim is separately patentable and it is requested that the obviousness rejection of this claim be overturned.

In regard to claim 18, this claim depends from independent claim 1 and incorporates the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 1, this claim is not obvious over Leon in view of Gravell. In addition, this claim includes the elements of "wherein the one or more commands corresponding to the importing shares state include commands for one or more of logon command, logoff command, query current user role command, query current user ID command, export transport public key command, import share command, combine shares command, set status command, session management commands, and audit entry creation command." The Examiner cites col. 8, line 63 - col. 9, line 19 of Leon as teaching these elements of claim 18. However, the cited section makes no mention of any of these commands, or any commands that correspond to exporting shares. Rather, the cited section of Leon relates to initialization transactions performed by a crypto-officer. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claim 18. Accordingly, it is believed that this claim is separately patentable and it is requested that the obviousness rejection of this claim be overturned.

In regard to claim 23, this claim depends from independent claim 1 and incorporates the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 1, this claim is not obvious over Leon in view of Gravell. In addition, this claim includes the elements of "wherein the cryptographic device includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user." The Examiner cites figs. 1A and 1B of Leon as teaching these elements of claim 23. However, the cited figures make no mention of support for multiple concurrent users with separate roles. Rather, the cited figures of Leon show only a single SMD being used in connection with a single PC. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claim 23. Accordingly, it is believed that this claim is separately patentable and it is requested that the obviousness rejection of this claim be overturned.

In regard to claims 28 and 30-33, these claims depend from independent claim 1 and incorporate the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 1, these claims are not obvious over Leon in view of Gravell. In addition, these claims include the elements of "wherein the value bearing item is" ... "a ticket," "a coupon," "currency," "a voucher" or "a traveler's check," respectively. The Examiner cites only fig. 9 of Leon as teaching these elements of claims 28 and 30-33. However, the cited figure makes does not depict any of these items. Rather, the cited figure of Leon depicts only a postage stamp. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claims 28 and 30-33. Accordingly, it is believed that these claims are separately patentable and it is requested that the obviousness rejections of these claims be overturned.

In regard to claim 34, this claim depends from independent claim 1 and incorporates the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 1, this claim is not obvious over Leon in view of Gravell. In addition, this claim includes the elements of " wherein each security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a

passphrase repetition list." The Examiner cites fig. 8F and table 3 in col. 42 of Leon as teaching these elements of claim 34. However, the cited figure and section does not teach security device transaction data with each of the elements listed. No mention is made of at least a passphrase repetition list, a last challenge received form a respective client subsystem, and user secrets. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claim 34. Accordingly, it is believed that this claim is separately patentable and it is requested that the obviousness rejections of this claim be overturned.

In regard to claim 36, this claim depends from independent claim 1 and incorporates the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 1, this claim is not obvious over Leon in view of Gravell. In addition, this claim includes the elements of "wherein the processor is capable of sharing a secret with a plurality of other cryptographic devices." The Examiner cites col. 13, lines 48-62 of Leon as teaching these elements of claim 36. However, the cited section makes no mention of sharing information between cryptographic devices. Rather the cited section of Leon relates to communication between a user PC and the SMD. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claim 36. Accordingly, it is believed that this claim is separately patentable and it is requested that the obviousness rejection of this claim be overturned.

In regard to claim 41, this claim depends from independent claim 1 and incorporates the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 1, this claim is not obvious over Leon in view of Gravell. In addition, this claim includes the elements of "wherein at least one of the plurality of users is an enterprise account." The Examiner cites fig. 1 of Leon as teaching these elements of claim 41. However, the cited figure makes no mention of and does not depict an enterprise account. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claim 41. Accordingly, it is believed that this claim is separately patentable and it is requested that the obviousness rejection of this claim be overturned.

In regard to claims 2-5, 8-10, 14, 15, 19-22, 29, 35, and 37-40, these claims depend from independent claim 1 and incorporate the limitations thereof. Thus, at least for the reasons

mentioned in regard to claim 1, these claims are not obvious over the cited references. Accordingly, it is requested that the obviousness rejection of theses claims be overturned.

Claims 42, 72 and 104 contain elements similar to those of independent claim 1. Claim 42 includes the elements of "a plurality of remotely located users," "authenticating the plurality of users for secure processing of a value bearing item" and "determining a state in a state machine for availability of one or more commands." Claim 72 includes the elements of "a plurality of user terminals coupled to the computer network" and "a plurality of cryptographic devices remote from the plurality of user terminals and coupled to the computer network, wherein the plurality of cryptographic devices manages value available to users and includes a state machine for determining a state corresponding to one or more commands available to an authenticated user." Claim 104 includes the elements "one or more of a plurality of cryptographic devices remote from the plurality of user terminals, wherein each of the cryptographic devices manages value available for the value bearing items" and "determining a state in a state machine for availability of one or more commands." The Examiner offers identical citations to Leon as teaching each these elements of the independent claims as were offered for claim 1. Thus, at least for the reasons mentioned above in regard to claim 1, these claims are not taught or suggested by Leon in view of Gravell.

In addition, claims 42 includes the elements of "authenticating the plurality of users for secure processing ... *using one of a plurality of cryptographic devices.*" The Examiner has not indicated and the Appellants have been unable to discern any part of the cited references that teach these elements of claim 42. Thus, Appellants do not believe that either Leon or Gravell teach or suggest these elements of claim 42. Rather, Leon teaches a system with a single SMD at each user PC. As a result, there is a one to one ratio between users and SMDs. Gravell teaches a system with a single data center with a single key management server. See Fig. 1, and col. 6, line 47 - col. 7, line 37 of Gravell. Thus, the Examiner has failed to establish that the cited references teach these elements of claim 42. Therefore, this claim is separately patentable.

Claim 72 includes the elements of "a plurality of cryptographic devices remote from the plurality of user terminals ... wherein one of the plurality of cryptographic devices manages value available to the users." The Examiner has not indicated and the Appellants have been

unable to discern any part of the cited references that teach these elements of claim 72. Thus, Appellants do not believe that either Leon or Gravell teach or suggest these elements of claim 72. Rather, Leon teaches a system with a single SMD at each user PC. As a result, there is a one to one ratio between users and SMDs. Gravell teaches a system with a single data center with a single function server. See Fig. 1, and col. 6, line 47 - col. 7, line 37 of Gravell. Thus, the Examiner has failed to establish that the cited references teach these elements of claim 72. Therefore, this claim is separately patentable.

Claim 104 includes the elements of "securing the information about the users in the database by one or more of a plurality of cryptographic devices." The Examiner has not indicated and the Appellants have been unable to discern any part of the cited references that teach these elements of claim 104. Thus, Appellants do not believe that either Leon or Gravell teach or suggest these elements of claim 104. Rather, Leon teaches a system with a single SMD at each user PC. As a result, there is a one to one ratio between users and SMDs. Gravell teaches a system with a single data center with a single key management server. See Fig. 1, and col. 6, line 47 - col. 7, line 37 of Gravell. Thus, the Examiner has failed to establish that the cited references teach these elements of claim 104. Therefore, this claim is separately patentable.

In regard to claims 51, 52, 78, 79, 113 and 114 these claims depend from independent claims 42, 72 and 104, respectively, and incorporate the limitations thereof. Thus, at least for the reasons mentioned in regard to claims 42, 72 and 104, these claims are not obvious over Leon in view of Gravell. In addition, these claims include the elements of "an exporting shares state" and "an importing shares state." The sections of Leon relied upon by the Examiner do not mention such states or the use of shares. Thus, Appellants believe the Examiner has failed to establish that these elements of these claims are taught or suggested by the cited references. Accordingly, it is believed these claims are separately patentable and it is requested that the obviousness rejections of these claims be overturned.

In regard to claims 57 and 84, these claims depend from independent claims 42 and 72, respectively, and incorporate the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 42, these claims are not obvious over Leon in view of Gravell. In addition, these

claims include the elements of "wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access control database command, change password command, set clock command, and set Status command." The Examiner cites col. 8, lines 45-62 of Leon as teaching these elements of claims 57 and 84. However, the cited section makes no mention of any of these commands, or any commands that correspond to access control. Rather, the cited sections of Leon relate to support for a crypto-officer by an SMD. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claims 57 and 84. Accordingly, it is believed that these claims are separately patentable and it is requested that the obviousness rejections of these claims be overturned.

In regard to claims 58 and 85, these claims depend from independent claims 42 and 72, respectively, and incorporate the limitations thereof. Thus, at least for the reasons mentioned in regard to claims 42 and 72, these claims are not obvious over Leon in view of Gravell. In addition, these claims include the elements of "wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session MAC command, session encrypt command, and session decrypt command." The Examiner cites fig 5E and col. 17, lines 47-54 and col. 19, lines 33-42 of Leon as teaching these elements of claims 58 and 85. However, the cited section makes no mention of any of these commands or any commands that correspond to session management. Rather, the cited section of Leon relates to an Initialization transaction. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claims 58 and 85. Accordingly, it is believed that these claims are separately patentable and it is requested that the obviousness rejections of these claims be overturned.

In regard to claims 61 and 88, these claims depend from independent claims 42 and 72, respectively, and incorporate the limitations thereof. Thus, at least for the reasons mentioned in regard to claims 42 and 72, these claims are not obvious over Leon in view of Gravell. In addition, these claims include the elements of "wherein the one or more commands corresponding to the administrative state include commands for one or more of create account command, delete account command, modify account command, view access control database

command, end admin. command, logon command, logoff command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command." The Examiner cites col. 8, line 63 - col. 9, line 33 of Leon as teaching these elements of claims 61 and 88. However, the cited section makes no mention of any of these commands or any commands that correspond to an administrative state. Rather, the cited sections of Leon relate to initialization by a crypto-officer. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claims 61 and 88. Accordingly, it is believed that these claims are separately patentable and it is requested that the obviousness rejections of these claims be overturned.

In regard to claims 62 and 89, these claims depend from independent claims 42 and 72, respectively, and incorporate the limitations thereof. Thus, at least for the reasons mentioned in regard to claims 42 and 72, these claims are not obvious over Leon in view of Gravell. In addition, these claims include the elements of "wherein the one or more commands corresponding to the exporting shares state include commands for one or more of logon command, logoff command, query Current User Role command, query current user ID command, export share command, abort export command, get status command, session management commands, and audit entry creation command." The Examiner cites figs. 5A, col. 12, line 30-42 and col. 12, table 1 of Leon as teaching these elements of claims 62 and 88. However, the cited sections make no mention of any of these commands or any commands that correspond to exporting shares. Rather, the cited section of Leon relates to services available to different roles. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claims 62 and 88. Accordingly, it is believed that these claims are separately patentable and it is requested that the obviousness rejections of these claims be overturned.

In regard to claims 63 and 90, these claims depend from independent claims 42 and 72, respectively, and incorporate the limitations thereof. Thus, at least for the reasons mentioned in regard to claims 42 and 72, these claims are not obvious over Leon in view of Gravell. In addition, these claims include the elements of "wherein the one or more commands corresponding to the importing shares state include commands for one or more of logon

command, logoff command, query current user role command, query current user ID command, export transport public key command, import share command, combine shares command, set status command, session management commands, and audit entry creation command." The Examiner cites 5A, col. 12, line 30-42 and col. 12, table 1 of Leon as teaching these elements of claims 63 and 90. However, the cited section makes no mention of any of these commands or any commands that correspond to importing shares. Rather, the cited section of Leon relates to services available to different roles. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claims 63 and 90. Accordingly, it is believed that these claims are separately patentable and it is requested that the obviousness rejections of these claims be overturned.

In regard to claims 69, 71 and 99, these claims depend from independent claims 42 and 72, respectively, and incorporate the limitations thereof. Thus, at least for the reasons mentioned in regard to claims 42 and 72, these claims are not obvious over Leon in view of Gravell. In addition, these claims include the elements of "wherein the value bearing item is" ... "a ticket" or "a coupon." The Examiner cites only fig. 9 of Leon as teaching these elements of claims 69, 71 and 99. However, the cited figure makes does not depict any of these items. Rather the cited figure of Leon depicts only a postage stamp. Therefore, the Examiner has failed to establish that the cited references teach or suggest each of the elements of claims 69, 71 and 99. Accordingly, it is believed that these claims are separately patentable and it is requested that the obviousness rejections of these claims be overturned.

In regard to claim 94, this claim depends from independent claim 72 and incorporates the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 72, this claim is not obvious over Leon in view of Gravell. In addition, this claim includes the elements of "wherein the cryptographic device includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user." The Examiner cites figs. 1A and 1B of Leon as teaching these elements of claim 94. However, the cited figures make no mention of support for multiple concurrent users with separate roles. Rather, the cited figures of Leon show only a single SMD being used in connection with a single PC. Therefore, the Examiner has failed to establish that the cited references teach or suggest

each of the elements of claim 23. Accordingly, it is believed that this claim is separately patentable and it is requested that the obviousness rejections of this claim be overturned.

In regard to claim 103, this claim depends from independent claim 72 and incorporates the limitations thereof. Thus, at least for the reasons mentioned in regard to claim 72, this claim is not obvious over Leon in view of Gravell. In addition, this claim includes the elements of "wherein at least one of the plurality of users is an enterprise account." The Examiner has failed to even alleged that the cited references teach the elements of this claim, instead alleging that "Leon teaches a method or (*sic*) printing a ticket, a bar code, a coupon (*see fig. 9*)." Thus, the Examiner has failed to even allege that the cited references teach the elements of claim 103. Accordingly, it is believed that this claim is separately patentable and it is requested that the obviousness rejections of this claim be overturned.

In regard to claims 43-50, 53-56, 59, 60, 64-68, 70, 73-77, 80-83, 86, 87, 91-93, 95-98, 100-102, 105-112 and 115-119 these claims depend from independent claims 42, 72 and 104, respectively, and incorporate the limitations thereof. Thus, at least for the reasons mentioned in regard to claims 42, 72 and 104, these claims are not obvious over the cited references. Accordingly, it is requested that the obviousness rejection of theses claims be overturned.

Conclusion

Accordingly, it is submitted that the rejections of claims 1-120 based on 35 U.S.C. § 103 be overturned.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By _____
Jonathan S. Miller
Reg. No. 48,534
626/795-9900

JSM/rjl
JSM PAS658905.1-*-01/9/06 1:48 PM

8. CLAIMS APPENDIX

1. (Previously Presented) A cryptographic device for securing data on a computer network comprising:

a processor programmed to authenticate a plurality of users on the computer network for secure processing of a value bearing item, wherein the processor includes a state machine for determining a state corresponding to availability of one or more commands;

a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users;

a cryptographic engine for cryptographically protecting data; and

an interface for communicating with the computer network;

wherein the cryptographic device is located remotely from the plurality of users; and

wherein once the user is authenticated, the cryptographic device enters an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user.

2. (Original) The cryptographic device of claim 1, wherein the state machine includes an uninitialized state.

3. (Original) The cryptographic device of claim 1, wherein the state machine includes an initialized state.

4. (Original) The cryptographic device of claim 1, wherein the state machine includes an operational state.

5. (Original) The cryptographic device of claim 1, wherein the state machine includes an administrative state.

6. (Original) The cryptographic device of claim 1, wherein the state machine includes an exporting shares state.

7. (Original) The cryptographic device of claim 1, wherein the state machine includes an importing shares state.

8. (Original) The cryptographic device of claim 1, wherein the state machine includes an error state.

9. (Original) The cryptographic device of claim 2, wherein the one or more commands corresponding to the uninitialized state includes a command for start initializing.

10. (Original) The cryptographic device of claim 3, wherein the one or more commands corresponding to the initialized state includes commands for one or more of get status command, initialize access control database command, logon command, logoff command, query current user role command, query current user ID command, session management commands, audit entry creation command, generate master key set command, and generate transport key pair commands.

11. (Original) The cryptographic device of claim 4, wherein the one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support.

12. (Original) The cryptographic device of claim 11, wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command,

view access control database command, change password command, set clock command, and set Status command.

13. (Original) The cryptographic device of claim 11, wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session MAC command, session encrypt command, and session decrypt command.

14. (Original) The cryptographic device of claim 11, wherein the commands for key management include one or more of export transport public key command, start importing MKS command, create MKS shares command, generate MKS command, activate MKS command, delete dormant MKS command, global decrypt and MAC command, compute MAC command, verify MAC, and encryption and MAC translation commands.

15. (Original) The cryptographic device of claim 11, wherein the commands for audit support include one or more of create audit entry command, create audit key command, and export audit verification key command.

16. (Original) The cryptographic device of claim 5, wherein the one or more commands corresponding to the administrative state include commands for one or more of create account command, delete account command, modify account command, view access control database command, end admin. command, logon command, logoff command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command.

17. (Original) The cryptographic device of claim 6, wherein the one or more commands corresponding to the exporting shares state include commands for one or more of

logon command, logoff command, query Current User Role command, query current user ID command, export share command, abort export command, get status command, session management commands, and audit entry creation command.

18. (Original) The cryptographic device of claim 7, wherein the one or more commands corresponding to the importing shares state include commands for one or more of logon command, logoff command, query current user role command, query current user ID command, export transport public key command, import share command, combine shares command, set status command, session management commands, and audit entry creation command.

19. (Original) The cryptographic device of claim 8, wherein the one or more commands corresponding to the error state include commands for one or more of get status command, and access control queries command.

20. (Original) The cryptographic device of claim 1 further comprising computer executable code to keep track of a present operational state.

21. (Original) The cryptographic device of claim 1, wherein the processor is programmed to verify that the authenticated user is authorized to assume a role and perform a corresponding operation.

22. (Original) The cryptographic device of claim 1, wherein the cryptographic device includes a computer executable code for preventing unauthorized disclosure of data.

23. (Original) The cryptographic device of claim 1, wherein the cryptographic device includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user.

24. (Original) The cryptographic device of claim 1, wherein the value bearing item is a postage value including a postal indicium.

25. (Original) The cryptographic device of claim 24, wherein the postal indicium comprises a digital signature.

26. (Original) The cryptographic device of claim 24, wherein the postal indicium comprises a postage amount.

27. (Original) The cryptographic device of claim 24, wherein the postal indicium comprises an ascending register of used postage and descending register of available postage.

28. (Original) The cryptographic device of claim 1, wherein the value bearing item is a ticket.

29. (Original) The cryptographic device of claim 1, wherein the value bearing item includes a bar code.

30. (Original) The cryptographic device of claim 1, wherein the value bearing item is a coupon.

31. (Original) The cryptographic device of claim 1, wherein the value bearing item is currency.

32. (Original) The cryptographic device of claim 1, wherein the value bearing item is a voucher.

33. (Original) The cryptographic device of claim 1, wherein the value bearing item is a traveler's check.

34. (Previously Presented) The cryptographic device of claim 1, wherein each security device transaction data includes an ascending register value, a descending register value,

a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

35. (Original) The cryptographic device of claim 1, wherein each security device transaction data includes information to define the present operational state of the device.

36. (Original) The cryptographic device of claim 1, wherein the processor is capable of sharing a secret with a plurality of other cryptographic devices.

37. (Original) The cryptographic device of claim 1, wherein the processor and the cryptographic engine generate a master key set (MKS).

38. (Original) The cryptographic device of claim 37, wherein the MKS includes a Master Encryption Key (MEK) used to encrypt keys when stored outside the device.

39. (Original) The cryptographic device of claim 38, wherein the MKS further includes a Master Authentication Key (MAK) used to compute a DES MAC for signing keys when stored outside of the device.

40. (Original) The cryptographic device of claim 1, wherein the cryptographic engine is programmed to perform one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

41. (Original) The cryptographic device of claim 1, wherein at least one of the plurality of users is an enterprise account.

42. (Previously Presented) A method for securing data on a computer network including a plurality of remotely-located users comprising the steps of:

authenticating the plurality of users for secure processing of a value bearing item using one of a plurality of cryptographic devices;

storing security device transaction data in a memory for ensuring authenticity and authority of one of the plurality of users, wherein the security device transaction data is related to the one of the plurality of users;

determining a state in a state machine for availability of one or more commands; and

once the user is authenticated, entering an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user.

43. (Original) The method of claim 42 further comprising the step of printing the value bearing item.

44. (Original) The method of claim 42 further comprising the step of storing a plurality of security device transaction data in a database wherein, each transaction data is related to one of the plurality of users.

45. (Original) The method of claim 44 further comprising the step of loading a security device transaction data related to the cryptographic device when the user requests to operate on a value bearing item.

46. (Original) The method of claim 42 further comprising the steps of authenticating the identity of each user and verifying that the identified user is authorized to assume a role and to perform a corresponding operation.

47. (Original) The method of claim 42, wherein the step of determining a state comprises of determining an uninitialized state.

48. (Original) The method of claim 42, wherein the step of determining a state comprises of determining an initialized state.

49. (Original) The method of claim 42, wherein the step of determining a state comprises of determining an operational state.

50. (Original) The method of claim 42, wherein the step of determining a state comprises of determining an administrative state.

51. (Original) The method of claim 42, wherein the step of determining a state comprises of determining an exporting shares state.

52. (Original) The method of claim 42, wherein the step of determining a state comprises of determining an importing shares state.

53. (Original) The method of claim 42, wherein the step of determining a state comprises of determining an error state.

54. (Original) The method of claim 47, wherein the one or more commands corresponding to the uninitialized state includes a command for start initializing.

55. (Original) The method of claim 48, wherein the one or more commands corresponding to the initialized state includes commands for one or more of get status command, initialize access control database command, logon command, logoff command, query current user role command, query current user ID command, session management commands, audit entry creation command, generate master key set command, and generate transport key pair commands.

56. (Original) The method of claim 49, wherein the one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support.

57. (Original) The method of claim 56, wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access control database command, change password command, set clock command, and set Status command.

58. (Original) The method of claim 56, wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session MAC command, session encrypt command, and session decrypt command.

59. (Original) The method of claim 56, wherein the commands for key management include one or more of export transport public key command, start importing MKS command, create MKS shares command, generate MKS command, activate MKS command, delete dormant MKS command, global decrypt and MAC command, compute MAC command, verify MAC, and encryption and MAC translation commands.

60. (Original) The method of claim 56, wherein the commands for audit support include one or more of create audit entry command, create audit key command, and export audit verification key command.

61. (Original) The method of claim 50, wherein the one or more commands corresponding to the administrative state include commands for one or more of create account

command, delete account command, modify account command, view access control database command, end admin. command, logon command, logoff command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command.

62. (Original) The method of claim 51, wherein the one or more commands corresponding to the exporting shares state include commands for one or more of logon command, logoff command, query Current User Role command, query current user ID command, export share command, abort export command, get status command, session management commands, and audit entry creation command.

63. (Original) The method of claim 52, wherein the one or more commands corresponding to the importing shares state include commands for one or more of logon command, logoff command, query current user role command, query current user ID command, export transport public key command, import share command, combine shares command, set status command, session management commands, and audit entry creation command.

64. (Original) The method of claim 53, wherein the one or more commands corresponding to the error state include commands for one or more of get status command, and access control queries command.

65. (Original) The method of claim 42, further comprising the step of printing a postage value including a postal indicium.

66. (Original) The method of claim 65, wherein the postal indicium includes a digital signature.

67. (Original) The method of claim 65, wherein the postal indicium includes a postage amount.

68. (Original) The method of claim 65, wherein the postal indicium comprises an ascending register of used postage and descending register of available postage.

69. (Original) The method of claim 42, further comprising the step of printing a ticket.

70. (Original) The method of claim 42, further comprising the step of printing a bar code.

71. (Original) The method of claim 42, further comprising the step of printing a coupon.

72. (Previously Presented) A security system for securing data in a computer network comprising:

a plurality of user terminals coupled to the computer network;

a plurality of cryptographic device remote from the plurality of user terminals and coupled to the computer network, wherein one of the plurality of cryptographic devices manages value available to users and includes a state machine for determining a state corresponding to one or more commands available to an authenticated user; and

a plurality of security device transaction data for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user; and

wherein, once the user is authenticated, the cryptographic device enters an operational state in which it continues to authenticate the user for one or more transactions requested by the user.

73. (Previously Presented) The system of claim 72, wherein the security device transaction data related to a user is loaded into the one of the plurality cryptographic devices when the user requests to operate on a value bearing item.

74. (Original) The system of claim 72, wherein the state machine includes an uninitialized state.

75. (Original) The system of claim 72, wherein the state machine includes an initialized state.

76. (Original) The system of claim 72, wherein the state machine includes an operational state.

77. (Original) The system of claim 72, wherein the state machine includes an administrative state.

78. (Original) The system of claim 72, wherein the state machine includes an exporting shares state.

79. (Original) The system of claim 72, wherein the state machine includes an importing shares state.

80. (Original) The system of claim 72, wherein the state machine includes an error state.

81. (Original) The system of claim 74, wherein the one or more commands corresponding to the uninitialized state includes a command for start initializing.

82. (Original) The system of claim 75, wherein the one or more commands corresponding to the initialized state includes commands for one or more of get status command, initialize access control database command, logon command, logoff command, query current

user role command, query current user ID command, session management commands, audit entry creation command, generate master key set command, and generate transport key pair commands.

83. (Original) The system of claim 76, wherein the one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support.

84. (Original) The system of claim 83, wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access control database command, change password command, set clock command, and set Status command.

85. (Original) The system of claim 83, wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session MAC command, session encrypt command, and session decrypt command.

86. (Original) The system of claim 83, wherein the commands for key management include one or more of export transport public key command, start importing MKS command, create MKS shares command, generate MKS command, activate MKS command, delete dormant MKS command, global decrypt and MAC command, compute MAC command, verify MAC, and encryption and MAC translation commands.

87. (Original) The system of claim 83, wherein the commands for audit support include one or more of create audit entry command, create audit key command, and export audit verification key command.

88. (Original) The system of claim 77, wherein the one or more commands corresponding to the administrative state include commands for one or more of create account command, delete account command, modify account command, view access control database command, end admin. command, logon command, logoff command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command.

89. (Original) The system of claim 78, wherein the one or more commands corresponding to the exporting shares state include commands for one or more of logon command, logoff command, query Current User Role command, query current user ID command, export share command, abort export command, get status command, session management commands, and audit entry creation command.

90. (Original) The system of claim 79, wherein the one or more commands corresponding to the importing shares state include commands for one or more of logon command, logoff command, query current user role command, query current user ID command, export transport public key command, import share command, combine shares command, set status command, session management commands, and audit entry creation command.

91. (Original) The system of claim 80, wherein the one or more commands corresponding to the error state include commands for one or more of get status command, and access control queries command.

92. (Original) The system of claim 72 further comprising computer executable code to keep track of a present operational state.

93. (Original) The system of claim 72, wherein the processor is programmed to verify that the authenticated user is authorized to assume a role and perform a corresponding operation.

94. (Original) The system of claim 72, wherein the system includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user.

95. (Original) The system of claim 72, wherein the value bearing item is a postage value including a postal indicium.

96. (Original) The system of claim 95, wherein the postal indicium comprises a digital signature.

97. (Original) The system of claim 95, wherein the postal indicium comprises a postage amount.

98. (Original) The system of claim 95, wherein the postal indicium comprises an ascending register of used postage and descending register of available postage.

99. (Original) The system of claim 72, wherein the value bearing item is a ticket.

100. (Original) The system of claim 72, wherein the value bearing item includes a bar code.

101. (Original) The system of claim 72, wherein each security device transaction data includes information to define the present operational state of the device.

102. (Original) The system of claim 72, wherein the cryptographic engine is programmed to perform one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

103. (Original) The system of claim 72, wherein at least one of the users is an enterprise account.

104. (Previously Presented) A method for secure printing of value-bearing items over a computer network having a plurality of user terminals, the method comprising the steps of:

storing information about a plurality of users using the plurality of terminals in a database remote from the plurality of user terminals;

securing the information about the users in the database by one or more of a plurality of cryptographic devices remote from the plurality of user terminals, wherein each of the cryptographic devices manages value available for the value bearing items;

storing a plurality of security device transaction data in the database, wherein each transaction data is related to one of the plurality of users; and

determining a state in a state machine for availability of one or more commands;

continuing to authenticate individual user transaction requests even after a user has been authorized by the cryptographic device.

105. (Original) The method of claim 104 further comprising the step of printing the value bearing item.

106. (Previously Presented) The method of claim 104 further comprising the step of loading a security device transaction data related to a user into one of the one or more of the plurality of cryptographic devices when the user requests to operate on a value bearing item.

107. (Original) The method of claim 104 further comprising the step of loading a security device transaction data related to the cryptographic device when the user requests to operate on a value bearing item.

108. (Original) The method of claim 104 further comprising the steps of authenticating the identity of each user and verifying that the identified user is authorized to assume a role and to perform a corresponding operation.

109. (Original) The method of claim 104, wherein the step of determining a state comprises of determining an uninitialized state.

110. (Original) The method of claim 104, wherein the step of determining a state comprises of determining an initialized state.

111. (Original) The method of claim 104, wherein the step of determining a state comprises of determining an operational state.

112. (Original) The method of claim 104, wherein the step of determining a state comprises of determining an administrative state.

113. (Original) The method of claim 104, wherein the step of determining a state comprises of determining an exporting shares state.

114. (Original) The method of claim 104, wherein the step of determining a state comprises of determining an importing shares state.

115. (Original) The method of claim 104, wherein the step of determining a state comprises of determining an error state.

116. (Original) The method of claim 104, further comprising the step of printing a postage value including a postal indicium.

117. (Original) The method of claim 116, wherein the postal indicium includes a digital signature.

118. (Original) The method of claim 116, wherein the postal indicium includes a digital signature.

119. (Original) The method of claim 116, wherein the postal indicium includes a postage amount.

120. (Original) The method of claim 104, further comprising the step of printing a ticket.

9. EVIDENCE APPENDIX

none

10. RELATED PROCEEDING APPENDIX

none